

Rec'd PCTO 07 APR 2005

PCT/JP 03/08794 #3

日本国特許庁
JAPAN PATENT OFFICE

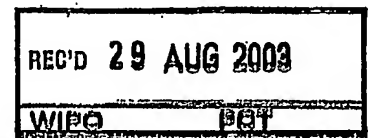
10.07.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2002年10月 7日

出願番号
Application Number: 特願2002-294184
[ST. 10/C]: [JP 2002-294184]



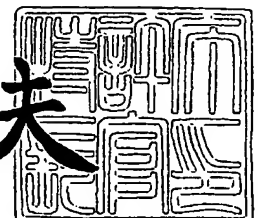
出願人
Applicant(s): 森井 昌克
小林 朗

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 8月15日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 P02-157
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
G06F 7/58

【発明者】
【住所又は居所】 徳島市助任本町 3 - 2 6
【氏名】 森井 昌克

【発明者】
【住所又は居所】 東大阪市新家中町 1 - 8 - 9 0 6
【氏名】 白石 善明

【特許出願人】
【住所又は居所】 徳島市助任本町 3 - 2 6
【氏名又は名称】 森井 昌克

【特許出願人】
【住所又は居所】 兵庫県西宮市上ヶ原四番町 4 番 3 3 - 7 0 8
【氏名又は名称】 小林 朗

【代理人】
【識別番号】 100100354
【弁理士】
【氏名又は名称】 江藤 聡明

【手数料の表示】
【予納台帳番号】 119438
【納付金額】 21,000円

【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 疑似乱数発生方法及び疑似乱数発生器

【特許請求の範囲】

【請求項1】 n 個のシフトレジスタを有し、1周期分のビット数が $(2^n - 1)$ 個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第1ステップと、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの1周期分のビット数と互いに素である導出値を求める第2ステップと、

該導出値と前記線形フィードバックシフトレジスタの1周期分のビット数を2倍以上した値とを乗算して、前記第1線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第3ステップと、

前記算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させる第4ステップと、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する第5ステップと、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する第6ステップと、

該再構成した後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる第7ステップと、

を有することを特徴とする疑似乱数発生方法。

【請求項2】 前記初期値に対してハッシュ関数を施してハッシュ値を求め、該ハッシュ値に最も近似した素数を導出値として採用することを特徴とする請求項1に記載の疑似乱数発生方法。

【請求項3】 前記線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする請求項1または2に記載の疑似乱数発生方法。

【請求項4】 前記第7ステップで発生させた疑似乱数を非線形変換する第8ステップを有することを特徴とする請求項1～3のいずれかに記載の疑似乱数発生方法。

【請求項 5】 n 個のシフトレジスタを有し、1 周期分のビット数が $(2^n - 1)$ 個となるビット列を出力可能な線形フィードバックシフトレジスタと、

秘密鍵に基づき前記線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの 1 周期分のビット数と互いに素である導出値を求める導出値算出手段と、

前記線形フィードバックシフトレジスタの 1 周期分のビット数を 2 倍以上した値と前記導出値とを乗算して、前記第 1 線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、

前記算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させるビット列出力手段と、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、

該再構成後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする疑似乱数発生器。

【請求項 6】 前記線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第 2 の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、

前記疑似乱数発生手段は、前記第 2 の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする請求項 5 に記載の疑似乱数発生器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、疑似乱数発生方法及び疑似乱数発生器に関し、特に暗号通信やデジタル署名などで利用する疑似乱数を発生させる疑似乱数発生方法及び疑似乱数発

生器に関する。

【0002】

【従来技術】

従来より、有線や無線により情報通信を行う際に、内容が第三者に漏れないように情報を暗号化して送信することが行われている。この暗号化方式の一つに逐次暗号方式（ストリーム暗号方式）がある。逐次暗号方式は、送信側と受信側で同一の疑似乱数を発生させ、送信側は疑似乱数のビット列と平文のビット列とを用いて暗号文のビット列を作成し暗号文として受信側に送出し、受信側は送信側から受信した暗号文のビット列と疑似乱数のビット列とを用いて平文のビット列を求め平文に復号化するものである。

【0003】

図4は、従来の逐次暗号方式を説明する図である。送信側の暗号化装置100は、疑似乱数発生器101と論理演算処理部102を有しており、受信側の復号化装置110は、疑似乱数発生器111と論理演算処理部112を有している。

【0004】

暗号化装置100の疑似乱数発生器101と復号化装置110の疑似乱数発生器111は、同一の秘密鍵を与えることによって互いに全く同一の疑似乱数を発生する論理構造を有している。また、暗号化装置100の論理演算処理部102と復号化装置110の論理演算処理部112は、ビット単位で排他的論理和の演算処理を行う。

【0005】

図5は、暗号化装置100の疑似乱数発生器101を説明する図である。尚、復号化装置110の疑似乱数発生器111については、暗号化装置100の疑似乱数発生器101と同一の構成を有するのでその詳細な説明を省略する。

【0006】

疑似乱数発生器101は、非線形コンバイナ型の疑似乱数発生器であり、図5に示すように、並列に配置した複数の線形フィードバックシフトレジスタ（LFSR）103と、非線形変換部104とを有しており、各線形フィードバックシフトレジスタ103から出力したビット列を非線形変換して疑似乱数を発生させ

る。本従来例では、各線形フィードバックシフトレジスタ103は、1回のシフト動作でそれぞれ1ビット (X_1 、 X_2 、 \dots X_L) を出力し、非線形変換部104は、各線形フィードバックシフトレジスタ103から入力されたビット列をもとに1ビットの疑似乱数を出力する構成を有している。

【0007】

図6は、一般的な線形フィードバックシフトレジスタ103の構成を簡単に説明する図である。線形フィードバックシフトレジスタ103は、1ビットの情報を記憶できる複数のシフトレジスタ105と、複数の排他的論理和演算回路106とを有し、各シフトレジスタ105の出力と各排他的論理和演算回路106の一方の入力との間にはフィードバックタップ107が接続されている。フィードバックタップ107 (c_{n-1} 、 c_{n-2} 、 \dots c_n) は、1のとき結線を示し、0のとき断線を示し、それぞれが予め1または0に定められている。

【0008】

このシフトレジスタ105の個数を n とすると、1つのシフトレジスタ105に注目したとき、出力系列の最大周期は、 $(2^n - 1)$ となることが知られており、この系列をM系列という。例えば、図6に示す線形フィードバックシフトレジスタ103の場合、M系列を生成する特性多項式は、以下の式で表される。

【0009】

$$C(x) = X^n + c_{n-1}X^{n-1} + \dots + c_1X + 1$$

上記の特性多項式で第1項目の指数 n は線形フィードバックシフトレジスタの次数、すなわちシフトレジスタの個数を示し、2項目以降の指数部分は、フィードバックタップによる結線位置を示している。上記(1)式に示す特性多項式が原始多項式となるようにすれば、線形フィードバックシフトレジスタは、M系列を出力する。

【0010】

尚、従来より、線形フィードバックシフトレジスタからの出力を排他的論理和等の演算処理によって変更することが提案されている（例えば、特許文献1参照。）。

【0011】

【特許文献 1】

特開平 6-342257 号

【0012】

【発明が解決しようとする課題】

しかしながら、線形フィードバックシフトレジスタ 103 は、シフトレジスタ数の 2 倍の出力を観測することで、線形フィードバックシフトレジスタ 103 の構成、すなわちシフトレジスタ数及び結線位置と、初期値の全てを特定することが可能である。したがって、構成が固定された線形フィードバックシフトレジスタ 103 をそのまま疑似乱数発生器 101 に用いるには、暗号強度が弱く、安全性に問題がある。

【0013】

また、線形フィードバックシフトレジスタ 103 は、特性多項式の変更によりシフトレジスタの結線位置や結線数を変更すると、線形フィードバックシフトレジスタの出力が M 系列ではなく短周期となって暗号強度が低下するおそれがあることから、特性多項式は予め M 系列を出力する値に固定されているのが常識であり、線形フィードバックシフトレジスタの構成を容易に変更することはできないと考えられている。

【0014】

本発明は、上述の点に鑑みなされたものであり、その目的は、強い暗号強度を維持しつつ線形フィードバックシフトレジスタの構成を容易かつ動的に変更することができる疑似乱数発生方法及び疑似乱数発生器を提供することにある。

【0015】

【課題を解決するための手段】

上記課題を解決する請求項 1 に記載の発明による疑似乱数発生方法は、 n 個のシフトレジスタを有し、1 周期分のビット数が $(2^n - 1)$ 個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第 1 ステップと、所定の演算処理により初期値から線形フィードバックシフトレジスタの 1 周期分のビット数と互いに素である導出値を求める第 2 ステップと、導出値と線形フィードバックシフトレジスタの 1 周期分のビット数を 2 倍以上した値とを乗算

して、第1線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第3ステップと、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させる第4ステップと、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する第5ステップと、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する第6ステップと、再構成した後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる第7ステップと、を有することを特徴とする。

【0016】

請求項2の発明は、請求項1に記載の疑似乱数発生方法において、初期値に対してハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数を導出値として採用することを特徴とする。

【0017】

請求項3の発明は、請求項1または2に記載の疑似乱数発生方法において、線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする。

【0018】

請求項4の発明は、請求項1～3のいずれかに記載の疑似乱数発生方法において、第7ステップで発生させた疑似乱数を非線形変換する第8ステップを有することを特徴とする。

【0019】

請求項5に記載の発明による疑似乱数発生器は、 n 個のシフトレジスタを有し、1周期分のビット数が $(2^n - 1)$ 個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により初期値から線形フィードバックシフトレジスタの1周期分のビット数と互いに素である導出値を求める導出値算出手段と、線形フィードバックシフトレジスタの1周期分のビット数を2倍以上した値と導出値とを乗算して、第1線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、その

算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させるビット列出力手段と、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、再構成後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする。

【0020】

請求項6に記載の発明は、請求項5に記載の疑似乱数発生器において、線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第2の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、疑似乱数発生手段は、第2の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする。

【0021】

【発明の実施の形態】

次に、本発明の実施の形態について図に基づいて説明する。

【0022】

図1は、本実施の形態における疑似乱数発生器1を説明する図である。本実施の形態では、非線形コンバイナ型の疑似乱数発生器1を例に説明する。

【0023】

疑似乱数発生器1は、利用者から与えられる秘密鍵に基づいて初期値を設定する初期値設定部（図示せず）と、初期値設定部から受け取った初期値をもとに疑似乱数を生成する複数の疑似乱数生成部10と、これら複数の疑似乱数生成部10の出力側に各々接続され、各疑似乱数生成部10から出力される疑似乱数を非線形変換する非線形変換部20を有している。

【0024】

初期値設定部は、利用者から与えられる秘密鍵をビット列に変換し、疑似乱数生成部10の数に分割して、後述する疑似乱数生成部10の線形フィードバック

シフトレジスタ 11 にそれぞれ割り当てる初期値を生成する処理を行う。

【0025】

疑似乱数生成部 10 は、L 個が互いに並列に配置されており、それぞれ線形フィードバックシフトレジスタ 11 と、線形フィードバックシフトレジスタ再構成手段 12 を有している。

【0026】

線形フィードバックシフトレジスタ 11 は、従来技術で説明したものと同様に、1 ビットの情報を記憶できる n 個のシフトレジスタと、排他的論理和演算回路を有している。そして、本実施の形態では、1 周期分のビット数 m が $(2^n - 1)$ 個となるビット列、いわゆる M 系列を出力可能な構成に予め設定されている。

【0027】

図 2 は、本実施の形態における線形フィードバックシフトレジスタ 11 の初期多項式を例示するものである。初期多項式は、M 系列を出力するように予め設定されている特性多項式であり、1 項目の指数部（図 2 では「 \wedge 」で表している）がシフトレジスタの個数を示し、2 項目以降の指数部が排他的論理和演算回路に接続された結線位置を示している。例えば、1 段目の線形フィードバックシフトレジスタ 11（LFSR1）は、131 個のシフトレジスタを有し、8 番目、3 番目、2 番目のシフトレジスタがフィードバックタップによって排他的論理和演算回路に接続されていることを示している。尚、本実施の形態では、シフトレジスタの個数 n は、全て素数個に設定されている。

【0028】

線形フィードバックシフトレジスタ再構成手段 12 は、線形フィードバックシフトレジスタ 11 の構成を秘密鍵によって動的に変更して再構成するものである。具体的には、出力系列が M 系列のビット列を s 個ごとにサンプルした新ビット列は、M 系列の 1 周期分のビット数 m ($= 2^n - 1$) と導出値 s とが互いに素であるとき、すなわち、1 以外の共通の約数を持たないときは、他の構成を有する線形フィードバックシフトレジスタの M 系列になり、また、バーレイキャンプマッセイアルゴリズムによって、少なくとも 2 周期分以上のビット数を有するビット列から、そのビット列を出力可能な等価で最小の線形フィードバックシフトレ

ジスタの特性多項式を求めることができることを利用して、線形フィードバックシフトレジスタ 11 の再構成を行う。

【0029】

線形フィードバックシフトレジスタ再構成手段 12 は、初期値設定部によって与えられた初期値から導出値 s を算出し、導出値 s と線形フィードバックシフトレジスタ 11 の 1 周期分のビット数 m ($= 2^n - 1$) を 2 倍した値 $2m$ とを乗算し、線形フィードバックシフトレジスタ 11 から出力させるビット列のビット数 $2ms$ を算出する。

【0030】

そして、初期値をもとに線形フィードバックシフトレジスタ 11 から $2ms$ 個のビット列を出力させ、その $2ms$ 個のビット列から導出値 s の間隔ごとにビット列を取り出して新ビット列を生成し、その新ビット列を用いてバーレイキャンプマッセイアルゴリズムにより線形フィードバックシフトレジスタ 11 の構成を変更する。

【0031】

尚、本実施の形態では、線形フィードバックシフトレジスタ 11 から出力させるビット列のビット数が $2ms$ 個である場合を例に説明しているが、新ビット列のビット数が $2m$ 個以上であれば、等価な最小の線形フィードバックシフトレジスタを求めることができるので、 $2ms$ 個以上であればよい。

【0032】

バーレイキャンプマッセイアルゴリズムとは、線形フィードバックシフトレジスタ 11 のシフトレジスタの個数 n (線形複雑度) の 2 倍以上のビット数を有するビット列を入手することで、そのビット列を出力可能な等価な最小の線形フィードバックシフトレジスタを得ることができるというアルゴリズムである。バーレイキャンプマッセイアルゴリズムについては、例えば、文献 1 「暗号理論入門 (第 2 版)」、共立出版社、岡本栄司著、2002 年 4 月 10 日発行、に詳細に説明されている。

【0033】

次に、上記構成を有する疑似乱数発生器 1 の動作について図 3 のフローチャー

トを用いて以下に説明する。

【0034】

まず最初に、初期値設定部によって初期値が設定される（ステップS101）。初期値は、利用者から与えられる秘密鍵を所定の演算処理によって分割することによって設定される。

【0035】

例えば、秘密鍵の長さが16バイトで「ABCDEFGHIJKLMNOP」であり、疑似乱数生成部10が8段の場合には、初期値は下記のように設定される。

【0036】

LFSR1 AB+X' FF' 埋め込み文字 (Padding)
LFSR2 CD+X' FF' 埋め込み文字 (Padding)
LFSR3 EF+X' FF' 埋め込み文字 (Padding)
LFSR4 GH+X' FF' 埋め込み文字 (Padding)
LFSR5 IJ+X' FF' 埋め込み文字 (Padding)
LFSR6 KL+X' FF' 埋め込み文字 (Padding)
LFSR7 MN+X' FF' 埋め込み文字 (Padding)
LFSR8 OP+X' FF' 埋め込み文字 (Padding)

ここでは、初期値は、秘密鍵「ABCDEFGHIJKLMNOP」を、「AB」、「CD」、・・・、「OP」の2文字ずつに分割し、残りのシフトレジスタを埋め込み文字 (Padding) で埋めることによって設定される。

【0037】

初期値設定部において秘密鍵から初期値が設定されると、各初期値は、各疑似乱数生成部10にそれぞれ入力され、線形フィードバックシフトレジスタ11のシフトレジスタ内にセットされる。

【0038】

次に、線形フィードバックシフトレジスタ再構成手段12によって、線形フィードバックシフトレジスタ11の構成を再構成する処理が行われる（ステップS102～ステップS106）。

【0039】

ここでは、まず、所定の演算処理により初期値から線形フィードバックシフトレジスタ11の1周期分のビット数 m と互いに素である導出値 s を算出する（ステップS102）。導出値 s は、初期値に対して、例えばMD5などのハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数が採用される。導出値 s は、初期値から求めることができ、かつビット数 m と互いに素であればよく、上記の算出方法によって求められるものに限定されない。但し、秘匿性を維持するために、上記所定の演算処理は、一方向性を満足しうる演算処理でなければならない。

【0040】

導出値 s を算出すると、次に、線形フィードバックシフトレジスタ11から出力させるビット列のビット数 $2ms$ を算出する（ステップS103）。線形フィードバックシフトレジスタ11から出力させるビット列のビット数 $2ms$ は、線形フィードバックシフトレジスタ11の1周期分のビット数 m （ $=2^n-1$ ）を2倍した値と、導出値 s とを乗算することによって求められる。

【0041】

そして次に、線形フィードバックシフトレジスタ11から初期値をもとに $2ms$ 個のビット数を有するビット列を出力させ（ステップS104）、そのビット列から新ビット列を生成する（ステップS105）。新ビット列は、 $2ms$ 個のビット列から導出値 s の間隔ごとに取り出したビット列によって構成され、そのビット数は $2m$ 個となる。

【0042】

ここで、出力系列がM系列のビット列を s 個ごとにサンプルしたビット列は、そのM系列の1周期分のビット数 m と導出値 s とが互いに素であれば、他の構成を有する線形フィードバックシフトレジスタのM系列となることから、この新ビット列も、M系列となる。

【0043】

そして、その新ビット列に基づいて線形フィードバックシフトレジスタ11の構成を再構成する（ステップS106）。線形フィードバックシフトレジスタ1

1の再構成は、バーレイキャンブマッセイアルゴリズムを用いて行われる。バーレイキャンブマッセイアルゴリズムによれば、少なくとも2周期分以上のビット数を有するビット列があれば、かかるビット列を出力可能な等価で最小の線形フィードバックシフトレジスタを求めることができるので、 2^m 個のビット数を有する新ビット列から新たな線形フィードバックシフトレジスタの特性多項式を導出して、再構成を行う。

【0044】

再構成後の線形フィードバックシフトレジスタ11は、再構成前と同一の次数及び異なる結線の特性多項式を有し、同一の初期値を与えた場合に、再構成前と異なるM系列を出力可能な構成を有する。

【0045】

線形フィードバックシフトレジスタ再構成手段12による線形フィードバックシフトレジスタ11の再構成が終了すると、再構成された線形フィードバックシフトレジスタ11から初期値をもとに疑似乱数を発生させる処理が行われる（ステップS107）。これにより、疑似乱数生成部10から再構成前とは異なるM系列の疑似乱数が発生される。

【0046】

各疑似乱数生成部10から出力された疑似乱数は、それぞれ非線形変換部30に入力され、非線形変換部30で所定の非線形関数 $f(x)$ に基づいて非線形変換される（ステップS108）。これにより、疑似乱数に非線形性を与えることができ、暗号強度を更に向上させることができる。

【0047】

上記構成を有する疑似乱数発生器1によれば、線形フィードバックシフトレジスタ11の構成を初期値に基づいて容易かつ動的に変更することができ、変更後もM系列を出力させることができる。したがって、解読者は、再構成前の線形フィードバックシフトレジスタの構成を取得することができない。これにより、従来、線形フィードバックシフトレジスタの構成が既知であることを前提に成り立っていた既存の暗号解読法は、成立しなくなる。したがって、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

【0048】

尚、本発明は、上述の実施の形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々の変更が可能である。例えば、上述の実施の形態では、非線形コンバイナ型の疑似乱数発生器 1 を例に説明したが、非線形コンバイナ型でなく、線形フィードバックシフトレジスタを用いる疑似乱数発生器であればよく、例えばブロック型暗号方式に用いられる疑似乱数発生器に用いてもよい。

【0049】

また、上記のステップ S106 で、新ビット列に基づいて線形フィードバックシフトレジスタ 11 の構成を再構成する代わりに、新ビット列を出力可能な構成を有する第 2 の線形フィードバックシフトレジスタを生成し、ステップ S107 で、その第 2 の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させてもよい。これによれば、線形フィードバックシフトレジスタを 2 つに分けることができ、より秘匿性の向上を図ることができる。

【0050】

また、本実施の形態における疑似乱数発生器 1 は、ソフトウェアやハードウェアのいずれによって構成してもよい。

【0051】

【発明の効果】

以上説明したように、本発明に係る疑似乱数発生方法によれば、出力系列が M 系列のビット列を s 個ごとにサンプルしたビット列は、その M 系列の 1 周期分のビット数 $m (= 2^n - 1)$ と導出値 s が互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタの M 系列を構成し、また、少なくとも 2 周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用して、線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタから M 系列のビット列を出力させることができる。

【0052】

したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値

や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

【図面の簡単な説明】

【図 1】

本実施の形態における疑似乱数発生器を説明する図である。

【図 2】

本実施の形態における線形フィードバックシフトレジスタの初期多項式を例示するものである。

【図 3】

本実施の形態における疑似乱数発生器の動作を説明するフローチャートである。

【図 4】

従来の逐次暗号方式を説明する図である。

【図 5】

従来の非線形コンバイナ型の疑似乱数発生器を概略的に示す図である。

【図 6】

一般的な線形フィードバックシフトレジスタの構成及び動作を簡単に説明する図である。

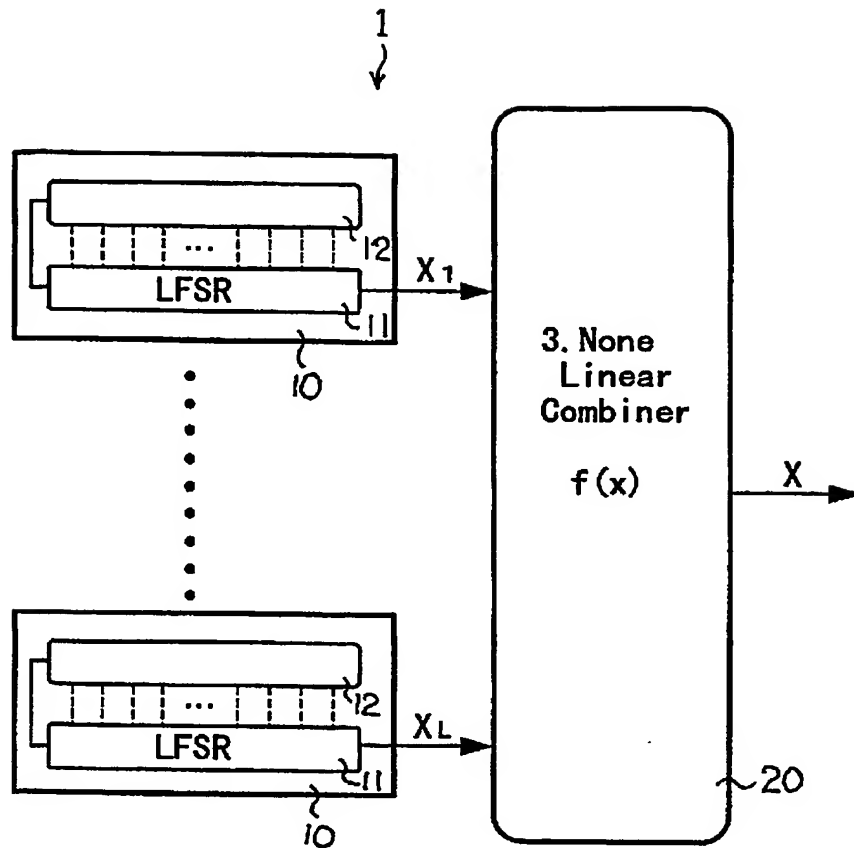
【符号の説明】

- 1 疑似乱数発生器
 - 10 疑似乱数生成部
 - 11 線形フィードバックシフトレジスタ
 - 12 線形フィードバックシフトレジスタ再構成手段
 - 20 非線形変換部

【書類名】

図面

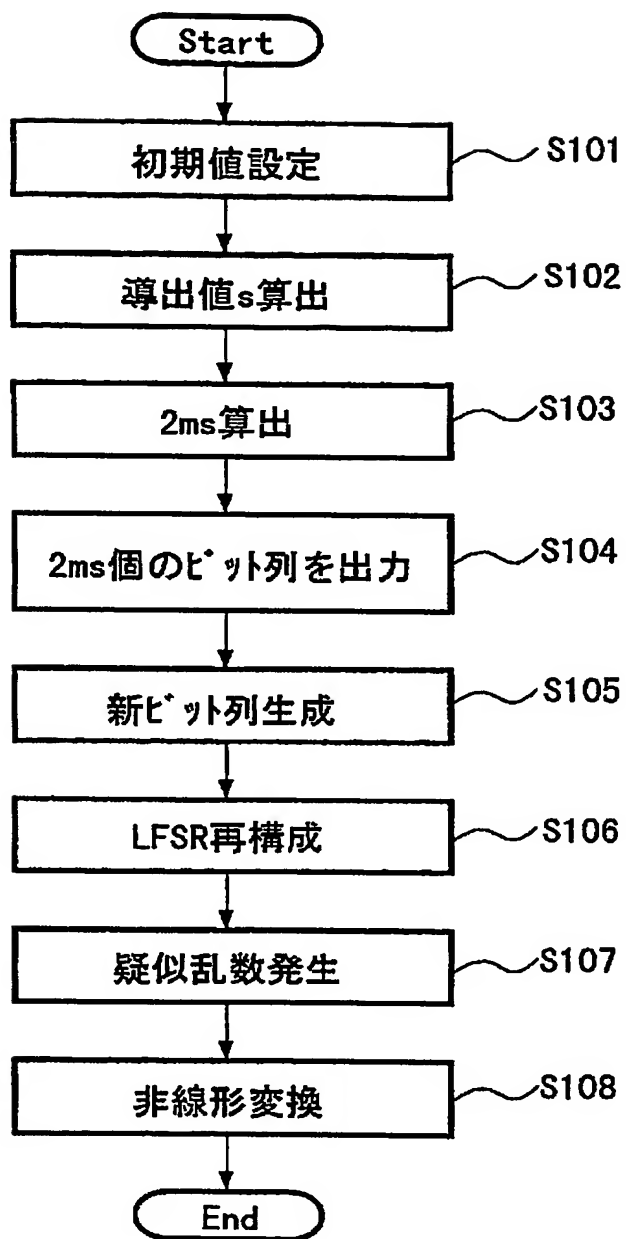
【図 1】



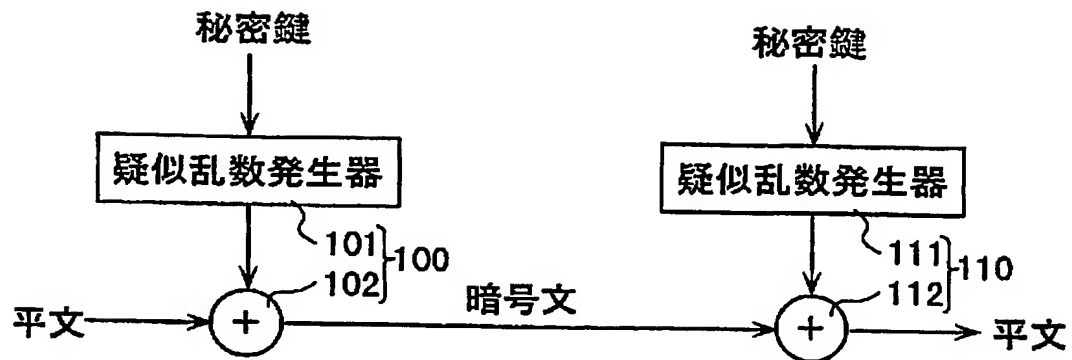
【図 2】

LSFR1	$x^{131} + x^8 + x^3 + x^2 + 1$
LSFR2	$x^{137} + x^{21} + 1$
LSFR3	$x^{139} + x^8 + x^5 + x^3 + 1$
LSFR4	$x^{149} + x^{10} + x^9 + x^7 + 1$
LSFR5	$x^{151} + x^3 + 1$
LSFR6	$x^{157} + x^6 + x^5 + x^2 + 1$
LSFR7	$x^{163} + x^7 + x^6 + x^3 + 1$
LSFR8	$x^{167} + x^6 + 1$

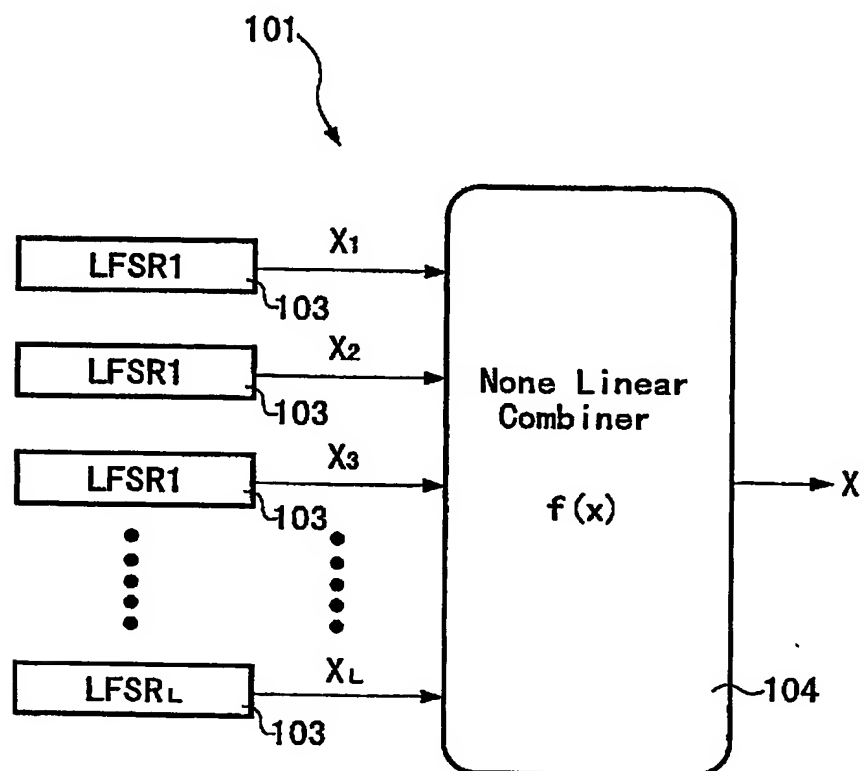
【図 3】



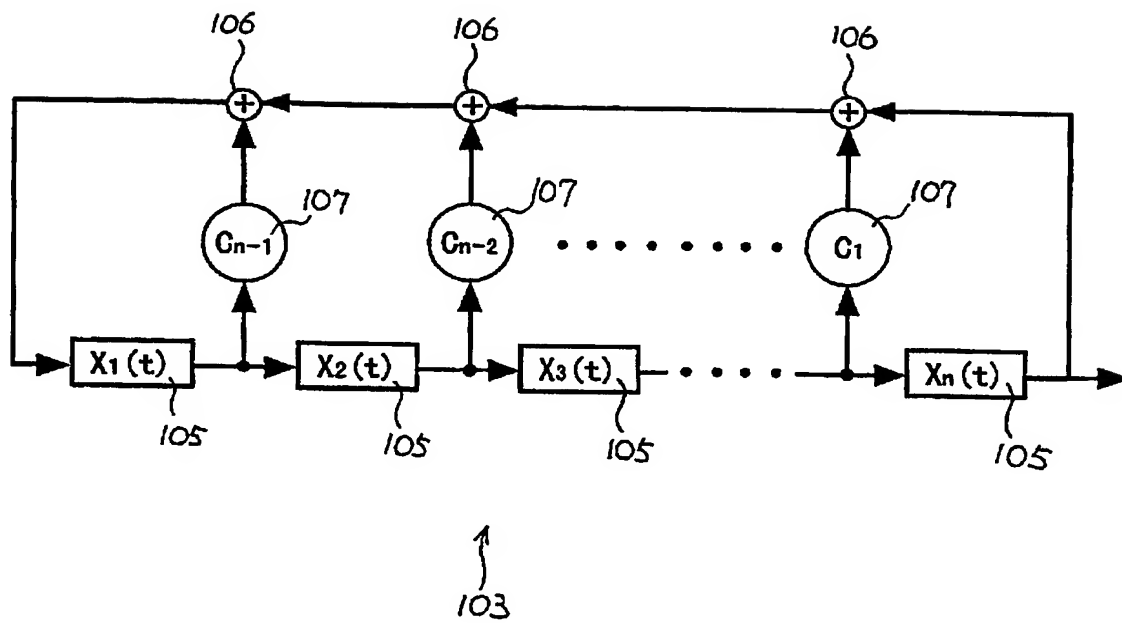
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 線形フィードバックシフトレジスタの構成を容易かつ動的に変更することができる疑似乱数発生方法を提供する。

を得ること。

【解決手段】 出力系列がM系列のビット列を s 個ごとにサンプルしたビット列は、そのM系列の1周期分のビット数 m と導出値 s が互いに素であるときは、他の構成を有する線形フィードバックシフトレジスタのM系列になり、また、少なくとも2周期分以上のビット数を有するビット列から最小で等価の線形フィードバックシフトレジスタを求めることができることを利用して、初期値に基づき線形フィードバックシフトレジスタ 11 の構成を容易かつ動的に変更する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2002-294184
受付番号	50201509791
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年10月10日

<認定情報・付加情報>

【提出日】	平成14年10月 7日
-------	-------------

次頁無

特願 2002-294184

出願人履歴情報

識別番号

[500030530]

1. 変更年月日 2000年 1月20日
 [変更理由] 新規登録
 住 所 徳島県徳島市助任本町326
 氏 名 森井 昌克

2. 変更年月日 2003年 5月28日
 [変更理由] 住所変更
 住 所 徳島県徳島市助任本町3-26
 氏 名 森井 昌克

特願 2002-294184

出願人履歴情報

識別番号

[502364800]

1. 変更年月日
[変更理由]

2002年10月 7日

住 所
氏 名

新規登録

兵庫県西宮市上ヶ原四番町4番33-708

小林 朗